



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,017	07/25/2003	John Mendonca	200209600-1	3688
22879	7590	02/14/2008	EXAMINER	
HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			OKORONKWO, CHINWENDU C	
			ART UNIT	PAPER NUMBER
			2136	
			NOTIFICATION DATE	DELIVERY MODE
			02/14/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/627,017	MENDONCA ET AL.	
Examiner	Art Unit		
Chinwendu C. Okoronkwo	2136		

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 13 November 2007.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-20 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892) 4) Interview Summary (PTO-413)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948) Paper No(s)/Mail Date. ____.
3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 5) Notice of Informal Patent Application
6) Other: ____.

DETAILED ACTION

Appeal Reopen

In view of the *appeal brief* filed on 11/13/2007, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,
- (2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:



Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being disclosed by Shanklin et al. (U.S. Patent No. 6,578,147 B1).

Regarding claims 1, 8 and 15, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for managing utilization of network intrusion detection systems in a dynamic data center, said method comprising: providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center (column 2 lines 48-50 – “Multiple intrusion detection sensors are used at the entry point to the network, specifically, at an ‘internetworking device’ such as a router or a switch” and column 2 lines 54-58 – “Internetworking device, whether a router or switch, is processor-based and includes load balancing programming, which controls how packets are distributed from the internetworking device to the sensors for

processing"); receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems (column 2 lines 1-13 – Shanklin et al. discloses the claimed "monitoring policy" as being inclusive to the IDS sensors, which comprise: "packet load to the sensors that is 'load balanced', such that said packets are distributed at least at a session-based level [or] packet-based level ... the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network"); and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy ("column 5 lines 19-20 – Shanklin et al. again discloses the "monitoring points" as being inclusive to the IDS sensors, which comprise "load balancing unit, which distributes packet among the sensors," which can be "session-based (column 5 line 22)" or "network-based (column 5 line 58)").

Shanklin et al. recites a local network "having a mesh topology ... [and] interconnected computer stations 10a, typically having a server 10b to function as a sort of gateway to network resources," which is equated to the dynamic data center mentioned in the preamble.

Shanklin et al. recites intrusion detection sensors which "autonomously comprise the entire intrusion detection system (column 3 lines 58-62).

Therefore, the Examiner understands the disclosed "multiple intrusion detection sensors" to comprise the function of claimed plurality of network intrusion detection system, monitoring points and monitoring policy. Thus the disclosure of Shanklin et al. highlights the various elements and components of the disclosed "multiple intrusion detection sensors are used at the entry point to the network, specifically, at an 'internetworking device' such as a router or a switch."

Regarding claims 2, 9 and 16, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for automatically arranging the monitoring of said monitoring points includes: automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems (column 3 lines 59-65 – "[sensors] might forward alarms to station 10c, which may then alert the system manager or automatically take action"); and automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy (column 2 lines 1-7 – "packet load to the sensors that is 'load balanced', such that said packets are distributed at least at a session-based level [or] packet-based level ... the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain

unauthorized access to the network).

Regarding claim 3, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for automatically arranging the monitoring of said monitoring points further includes: automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (column 2 lines 1-18 and column 3 lines 57-65 – the claimed automatically increasing IDS systems is found in the disclosure of the “solution provided by the invention [being] easily scalable” in size from large scale to small scale).

Regarding claims 4, 11 and 18, Shanklin et al., a method, system and a computer readable medium comprising computer-executable instructions stored therein for automatically arranging the monitoring of said monitoring points further includes: automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of

said particular network intrusion detection systems (column 2 lines 1-18 and column 3 lines 57-65 – the claimed automatically decreasing IDS systems is found in the disclosure of the “solution provided by the invention [being] easily scalable” in size from large scale to small scale

Regarding claims 5, 12 and 19, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for which resources include one of a firewall, a gateway system, a network switch, and a network router (column 1 lines 19-28 or column 3 lines 23-29).

Regarding claims 6 and 13, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for receiving a monitoring policy and a plurality of monitoring points to be monitored includes: providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored (column 3 lines 54-57 – “user interface”).

Regarding claims 7, 14, 20, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for which dynamic data center is a utility data center (column 1 lines 19-

26).

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CCO

February 1, 2008

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

2/3/08